PROCEDE ET SYSTEME D'ACCES CONDITIONNEL APPLIQUE A LA PROTECTION DE CONTENU

DESCRIPTION

DOMAINE TECHNIQUE

L'invention se situe dans le domaine du contrôle d'accès et concerne plus particulièrement un procédé et un système d'émission/réception d'informations avec contrôle d'accès à travers un réseau de diffusion MPEG2. Ce procédé est applicable à tout flux de données multiplexé reposant sur l'usage de paquet ou trame.

L'invention concerne également une plate-forme d'embrouillage et un récepteur de désembrouillage destinés à mettre en œuvre ce procédé.

Plus spécifiquement, l'invention concerne un procédé et un système de contrôle d'accès à un flux de données numériques diffusé et préalablement embrouillé par une clé de chiffrement CW transmise sous forme chiffrée dans un message de contrôle de titre d'accès ECM (pour "Entitlement Control Message") comportant au moins un critère CA de contrôle d'accès aux données du flux. Les données transmises étant susceptibles d'être déchiffrées à la volée ou enregistrées telles quelles dans un terminal récepteur.

ETAT DE LA TECHNIQUE ANTERIEURE

Afin de lutter contre le piratage de données et de services distribués en ligne, notamment via le réseau Internet, il devient primordial pour les

opérateurs de protéger ces données en phase de diffusion et après la diffusion.

La figure 1 représente un schéma général d'un système de contrôle d'accès de l'art antérieur dans lequel une plate-forme d'embrouillage 2, agencée généralement en tête de réseau, reçoit un flux en clair F_x et fournit à un terminal récepteur 4 un contenu chiffré F_{xs}. La plate-forme 2 comporte un générateur 6 de clés CWi d'embrouillage et de désembrouillage , un générateur messages de contrôle de titre d'accès (ECM) 8, et un générateur messages de gestion de titre d'accès (EMM) (pour "Entitlement Management Message) 10. Le terminal récepteur 4 comporte un module de désembrouillage 12, un processeur de sécurité 14 comportant un module de déchiffrage 16 des clés de contrôle CW_i et une mémoire 18.

Avant la diffusion des flux de données, ceux-ci sont embrouillés par la plate-forme d'embrouillage 2 au moyen des clés CWi. Afin de permettre le désembrouillage du contenu des flux diffusés, les clés de désembrouillage CW_i sont transmises aux terminaux 4 sous forme chiffrée dans les messages de contrôle de titre d'accès ECM avec au moins un critère CA de contrôle d'accès. Après vérification des critères d'accès au moyen d'un comparateur 20 à des droits préalablement transmis aux terminaux 4, dans les messages de gestion de titre d'accès (EMM) et inscrits dans la mémoire 18, les clés de désembrouillage CW_i sont déchiffrées puis transmises au module de désembrouillage 12.

Pour améliorer la sécurité globale du système, les clés de désembrouillage CW_i changent régulièrement sur des crypto-périodes CP_i (typiquement quelques secondes) et sont généralement appliquées au désembrouilleur 12 par couple $[CW_i, CW_{i+1}]$ où CW_i représentant la clé de désembrouillage valable pendant la crypto-période CP_i, et CW_{i+1} représentant la clé de désembrouillage valable pendant la crypto-période CP_{i+1}. Chaque clé de désembrouillage à utiliser est référencée par un bit indiquant la parité de i de sorte qu'à chaque changement d'ECM, deux clés de désembrouillage, une paire ECW et une impaire OCW, sont configurées sur le désembrouilleur avant le changement effectif de crypto-période.

Dans un contexte de télédiffusion, une technique connue pour protéger le contenu une fois diffusé consiste à enregistrer ce contenu avec la signalisation d'accès conditionnel associée.

Un premier inconvénient de cette solution provient du fait qu'elle ne permet pas d'associer des critères d'accès distincts pour les phases :

- de visualisation directe du contenu depuis le flux ;
- d'enregistrement du contenu ; et
- de visualisation du flux depuis le contenu enregistré localement.

Un second inconvénient de cette technique provient du fait que les clés secrètes d'exploitation stockées dans un processeur de sécurité et servant au déchiffrement des ECMs sont régulièrement mises à jour. Dans ce cas, les ECM stockés avec le contenu ne sont

plus valides et ce dernier devient inexploitable même si le client a acquis des droits d'utilisation dépassant cette période.

Un troisième inconvénient est lié aux aspects de synchronisation entre la fourniture et l'exploitation des clés de désembrouillage CW_i lors d'une exploitation d'un contenu enregistré. Dans ce cas, la fonction de lecture arrière ne peut pas être réalisée de manière simple, car la valeur anticipée de la prochaine clé de désembrouillage (représentant la clé de désembrouillage précédente) n'est pas fournie dans l'ECM.

Une autre technique connue dans l'art antérieur pour protéger le contenu est l'utilisation d'une solution dite DRM (pour Digital Right Management).

Ce type de solution repose sur :

- l'usage de certificats pour établir une chaîne de confiance entre les composants du système ;
- un chiffrement ou pré-embrouillage du contenu à l'aide d'un algorithme à clé privé ;
- l'envoi en ligne de cette clé privée associée aux droits d'utilisations pour former une licence chiffrée à l'aide d'un algorithme de chiffrement utilisant une clé publique du client.

Cette solution n'est pas adaptée au contexte de la télédiffusion dans lequel l'usage d'une voie de retour n'est pas systématique. De plus, ce type de solution ne permet pas de conditionner l'accès au contenu moyennant la possession de droits inscrits

indifféremment par voie hertzienne ou en ligne dans un processeur de sécurité.

Le but de l'invention est de pallier les inconvénients de l'art antérieur décrits ci-dessus au moyen d'un procédé et d'un dispositif utilisant un processus d'embrouillage basé sur des changements périodiques de mots de contrôle et assurant une compatibilité ascendante avec les systèmes d'accès conditionnel antérieurs.

EXPOSÉ DE L'INVENTION

L'invention préconise un procédé de contrôle d'accès à un flux de données numériques diffusé et préalablement embrouillé au moyen d'une clé de chiffrement CW transmise sous forme chiffrée dans un message de contrôle de titre d'accès ECM comportant en outre au moins un critère CA de contrôle d'accès, lesdites données numériques étant susceptibles d'être enregistrées telles quelles dans un terminal récepteur ou déchiffrées à la volée.

Selon l'invention, ce procédé comporte les étapes suivantes :

à l'émission :

- générer un message $R\text{-}ECM_c$ de contrôle de titre d'accès à l'enregistrement du contenu du flux en fonction d'une clé d'enregistrement KR_c et d'au moins un critère CRR définissant un droit à l'enregistrement,
- générer un message $P\text{-}ECM_c$ de contrôle de titre d'accès à la relecture du contenu du flux enregistré en fonction d'une clé de relecture KP_c et d'au moins

un critère CRP définissant un droit à la relecture, et

à la réception :

- analyser le message R-ECM_c, et
- autoriser l'enregistrement si le critère CRR est vérifié, sinon, interdire l'enregistrement,
- analyser le message P-ECM_c, et
- autoriser la relecture si le critère CRP est vérifié, sinon, interdire la relecture.

Selon une première variante de réalisation du procédé de l'invention, les clés CW, KR_c et KP_c sont chiffrées par une première clé de service K_s.

Selon une deuxième variante de réalisation du procédé de l'invention les clés CW, KR_c et KP_c sont chiffrées par trois clés de service différentes respectivement K_S, K_{SR} et K_{SP}.

Dans un premier mode de réalisation, la phase de l'émission comporte les étapes suivantes :

pour chaque flux de données

- découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i, et à chaque changement de crypto-période,

- embrouiller le contenu du flux au moyen de la clé CW_i, et mémoriser une valeur p(i) représentative de la parité de i,

- calculer un message de contrôle de titre d'accès SC-ECM_i en fonction des clés de chiffrement

CW_{i-1}, CW_i, CW_{i+1} préalablement définies, de la valeur p(i) et du critère CA_i, ledit message $SC\text{-}ECM_i$ étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,

- chiffrer les clés CW_{i-1}, CW_i, CW_{i+1} au moyen de la clé de relecture KP_c,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une deuxième clé de service K'_s,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé d'enregistrement KR_c.

Dans un deuxième mode de réalisation, la phase de l'émission comporte les étapes suivantes :

pour chaque flux de données :

- découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i, et, à chaque changement de crypto-période i,

- embrouiller le contenu du flux au moyen de la clé CW_i, et mémoriser une valeur p(i) représentative de la parité de i,

- calculer un message de contrôle de titre d'accès $SC\text{-}ECM_i$ en fonction des clés de chiffrement CW_{i-1}, CW_i, CW_{i+1} préalablement définies, de la valeur p(i) et du critère CA_i, ledit message $SC\text{-}ECM_i$ étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,

- chiffrer les clés CW_{i-1}, CW_i, CW_{i+1} au moyen d'une deuxième clé de service K'_s,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé de relecture KP_c,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé d'enregistrement KR_c.

Dans les deux modes de réalisation, la phase de l'émission comporte en outre les étapes consistant :

- calculer le message de contrôle de titre d'accès $ECM_i = f[(ECW_i, OCW_i, CA)]$ où, ECW_i et OCW_i représentent respectivement les mots de contrôle pair et impair préalablement chiffrés au moyen d'une première clé de service K_s,

$ECW_i = CW_i$ si i pair sinon $ECW_i = CW_{i+1}$;

$OCW_i = CW_i$ si i impair sinon $OCW_i = CW_{i+1}$;

- diffuser dans la signalisation ECM des paramètres identifiant les voies ECM rattachées au service diffusant le contenu des messages ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$,

- fournir au terminal récepteur les messages ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$

Deux modes de distribution des messages ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$ sont possibles. Ces derniers peuvent être soit diffusés sur la voie ECM associée au contenu du segment S_i, soit délivrés en partie au terminal récepteur à partir d'un Serveur

d'Autorisation en tête de réseau sur requête et en fonction du type d'exploitation du contenu envisagé.

Ainsi, les message R-ECM et/ou P-ECM peuvent être délivrés au terminal récepteur sur requête à partir d'un Serveur d'Autorisation en tête de réseau si l'enregistrement et/ou la relecture sont envisagés.

Selon l'invention, pour recevoir directement le flux reçu, la phase de la réception comporte les étapes suivantes :

- récupérer la voie ECM du message ECM_i à partir de la signalisation rattachée au service diffusant le flux de données, et à chaque changement de i,

- analyser le message ECM_i afin de récupérer les mots de contrôle pair OCW, et impair ECW, pour désembrouiller le contenu du flux diffusé de manière à obtenir un accès direct à ce contenu.

Pour enregistrer le flux reçu, la phase de la réception comporte les étapes suivantes :

- récupérer la voie ECM des messages $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$ à partir de la signalisation rattachée au service diffusant le contenu ;

- analyser le message $R\text{-}ECM_c$ pour vérifier les critères d'accès à l'enregistrement CRR

- mémoriser la clé d'enregistrement KR_c ;

- récupérer le message $P\text{-}ECM_c$ et le stocker avec le contenu ; et

pour chaque crypto-période i :

- récupérer le message $SC\text{-}ECM_i$,

- déchiffrer le message $SC\text{-}ECM_i$ au moyen de la clé d'enregistrement KR_c, et

- enregistrer le message $SC\text{-}ECM_I$ déchiffré avec le contenu.

Selon l'invention, l'accès à la relecture du contenu du flux enregistré est obtenu selon les étapes suivantes :

- récupérer le message $P\text{-}ECM_c$ dans le contenu et l'analyser pour vérifier les critères d'accès à la lecture CRP,
- mémoriser la clé de relecture KP_c ; et
- récupérer dans le contenu le message $SC\text{-}ECM_i$ courant ;
- déchiffrer le message $SC\text{-}ECM_i$ avec la clé de relecture KP_c et vérifier les critères d'accès,
- récupérer les clés chiffrées CW_{i-1}, CW_i, CW_{i+1} et la valeur p(i) indiquant la parité de i, et
- déchiffrer, au moyen de la deuxième clé K'_s, lesdites clés suivant le sens de lecture pour en déduire ECW et OCW ; puis,
- appliquer soit ECW, soit OCW pour désembrouiller le contenu à la relecture.

Dans une autre variante, l'accès à la relecture du contenu du flux est obtenu selon les étapes suivantes :

- récupérer le message $P\text{-}ECM_c$ dans le contenu,
- analyser le message $P\text{-}ECM_c$ pour vérifier les critères d'accès à la lecture CRP,
- mémoriser KP_c, et
- récupérer dans le contenu le message $SC\text{-}ECM_i$ courant,

- déchiffrer le message $SC\text{-}ECM_i$ avec la deuxième clé de service K'_S et vérifier les critères d'accès,

- récupérer les clés chiffrés CW_{i-1}, CW_i, CW_{i+1} et la valeur p(i) indiquant la parité de i, et

- déchiffrer, au moyen de la deuxième clé KRc lesdites clés suivant le sens de lecture pour en déduire ECW et OCW ; puis,

- appliquer soit ECW, soit OCW pour désembrouiller le contenu.

Préférentiellement, la phase de réception comporte en outre les étapes suivantes :

- générer une clé locale K_I à partir d'attributs contenus dans le message R-ECM et d'au moins un paramètre relatif à l'identité du terminal-récepteur,

- sur-chiffrer localement le contenu à enregistrer par cette clé K_I.

- à la relecture, regénérer la clé K_I à partir d'attributs contenus dans le message P-ECM et d'au moins un paramètre relatif à l'identité du terminal-récepteur,

- déchiffrer le contenu enregistré au moyen de la clé K_I regénérée.

Dans une application particulière du procédé selon l'invention, les données numériques diffusées représentent des programmes audiovisuels.

L'invention concerne également un système de contrôle d'accès à un flux de données numériques comportant une plate-forme d'embrouillage comprenant au moins un générateur de messages de contrôle de titre d'accès ECM et au moins un récepteur de désembrouillage muni d'un processeur de sécurité.

Selon l'invention, la plate-forme d'embrouillage comporte en outre:

- un générateur de messages $R\text{-}ECM_c$ de contrôle de titre d'accès à l'enregistrement du contenu du flux reçu et un générateur de messages $P\text{-}ECM_c$ de contrôle de titre d'accès à la relecture du contenu d'un flux enregistré, et le récepteur de désembrouillage comporte :

- des moyens pour récupérer la voie ECM des messages $P\text{-}ECM_c$, $R\text{-}ECM_c$,

- des moyens pour déchiffrer le contenu d'un flux reçu pour l'enregistrer,

- des moyens pour déchiffrer le contenu d'un flux enregistré pour le relire.

Préférentiellement, le récepteur de désembrouillage comporte en outre des moyens pour générer une clé locale K_I à partir d'attributs contenus dans le message R-ECM et de l'identité du terminal-récepteur pour chiffrer/déchiffrer localement le contenu du flux reçu.

L'invention concerne également une plate-forme d'embrouillage comportant au moins un générateur de messages de contrôle de titre d'accès ECM à un flux de donnée diffusé sous forme embrouillée, un générateur de messages $R\text{-}ECM_c$ de contrôle de titre d'accès à

l'enregistrement du contenu d'un flux reçu et un générateur de messages P-ECM_c de contrôle de titre d'accès à la relecture du contenu d'un flux enregistré.

La plate-forme d'embrouillage comporte en outre :

- des moyens pour découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i,
- des moyens pour chiffrer le contenu du flux à chaque changement de crypto-période i au moyen de la clé CW_i,
- des moyens pour calculer un message de contrôle de titre d'accès SC-ECM_i en fonction des clés CW_{i-1}, CW_i, CW_{i+1} correspondant respectivement aux crypto-périodes CP_i, CP_{i-1} et CP_{i+1}, d'un paramètre de parité p(i) et du critère de contrôle d'accès CA_i, ledit message SC-ECM_i étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,
- des moyens pour chiffrer les clés CW_{i-1}, CW_i, CW_{i+1} au moyen d'une clé de relecture KP_c,
- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une deuxième clé de service K'_s,
- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une clé d'enregistrement KR_c.

L'invention concerne également un récepteur de désembrouillage d'un flux de donné diffusé sous forme embrouillée par une clé d'embrouillage CW_i

comportant un processeur de sécurité dans lequel est mémorisée au moins une clé d'enregistrement KR_c destinée à désembrouiller des messages de contrôle d'accès à l'enregistrement $R\text{-}ECM_c$ et au moins une clé de relecture KP_c destinée à désembrouiller des messages de contrôle d'accès à la relecture $P\text{-}ECM_c$,

Selon l'invention, ce récepteur comporte :

- des moyens pour récupérer la voie ECM des messages $P\text{-}ECM_c$, et des messages $R\text{-}ECM_c$ à partir de la signalisation rattachée au service diffusant le contenu ;

- des moyens pour déchiffrer le message $R\text{-}ECM_c$ au moyen de la clé d'enregistrement KR_c pour vérifier le droit à enregistrer le contenu d'un flux reçu,

- des moyens pour déchiffrer le message $P\text{-}ECM_c$ au moyen de la clé de relecture KP_c pour vérifier le droit à relire le contenu d'un flux enregistré,

Préférentiellement, le récepteur selon l'invention comporte en outre des moyens pour générer une clé K_I à partir de l'identité du récepteur pour chiffrer et déchiffrer localement le contenu du flux reçu.

Dans un mode de réalisation préféré de l'invention, le processeur de sécurité est une carte à puce.

BRÈVE DESCRIPTION DES DESSINS

D'autres caractéristiques et avantages de l'invention ressortiront de la description qui va

suivre, prise à titre d'exemple non limitatif, en référence aux figures annexées dans lesquelles :

- la figure 1, décrite précédemment, représente un schéma général d'un système de contrôle d'accès de l'art antérieur ;
- la figure 2 représente un schéma bloc illustrant la phase d'embrouillage des flux à diffuser par un système de contrôle d'accès selon l'invention,
- la figure 3 illustre schématiquement le processus de contrôle d'accès à l'enregistrement d'un flux de données selon l'invention,
- la figure 4 illustre schématiquement le processus de contrôle d'accès à la relecture du flux de données enregistré selon l'invention.

EXPOSÉ DÉTAILLÉ DE MODES DE RÉALISATION PARTICULIERS

La description qui suit sera faite dans le cadre d'une application particulière dans laquelle les flux diffusés représentent des programmes audiovisuels nécessitant un droit d'accès.

Dans cette application, le procédé repose sur une diffusion de contenu à travers une structure de paquets multiplexés dont la forme est indiquée à l'annexe 1.

La signalisation du programme diffusant le contenu comprend une description précise indiquant les voies du multiplex par un identifiant de paquet « Packet Identifier » en anglais utiles à la réception du contenu ainsi que la nature des données transmise dans chaque voie (composante son, vidéo ou autre).

Cette signalisation comprend un descripteur d'accès conditionnel "CA_descriptor" indiquant la présence et la localisation des voies transportant les ECMs. Ce descripteur est associé soit au niveau global du programme, soit au niveau de chaque déclaration d'une voie composante.

Le format de ce descripteur est standard dans le cas d'une diffusion MPEG2 ISO13818-1 représenté à l'annexe 2.

Les données privées "private_data_byte" pour le procédé décrit sont décrites dans l'annexe 3 pour un mode de réalisation.

Elles ont un suffixe XID dans l'entête des ECMs et servent de discriminant pour distinguer les ECM véhiculés éventuellement sur la même voie paquet.

Lorsqu'une partie des voies ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$ est absente, les combinaisons possibles sont les suivantes :

- voie ECM_i absente : pas de visualisation immédiate ;
- voie $R\text{-}ECM_c$ absente : enregistrement interdit ou si le terminal récepteur dispose d'une voie de retour opérationnelle, se connecter à un Serveur d'Autorisation en tête de réseau délivrant le message $R\text{-}ECM_c$ nécessaire à l'enregistrement du contenu ;
- voie $P\text{-}ECM_c$ absente : lecture interdite ou si le terminal récepteur dispose d'une voie de retour opérationnelle, se connecter à un Serveur d'Autorisation en tête de réseau délivrant le message $P\text{-}ECM_c$ nécessaire à la lecture du contenu enregistré;
- voie $SC\text{-}ECM_i$ absente : alors $R\text{-}ECM_i$ et $P\text{-}ECM_i$ sont absentes et l'enregistrement n'est pas autorisé.

Selon la nature des données transmises, signalisation ou composante audio ou son, la charge utile « payload » en anglais est chiffrée ou non par la plate-forme d'embrouillage 2 et la valeur du champ "Scrambling Control" prend les valeur suivantes :

- le paquet n'est pas embrouillé,
- le paquet est embrouillé par le mot de contrôle pair ECW,
- le paquet est embrouillé par le mot de contrôle impair OCW.

La figure 2 illustre schématiquement la phase d'embrouillage des flux à diffuser par un système de contrôle d'accès selon l'invention.

L'étape 30 consiste à générer une clé secrète d'enregistrement KR_c de contrôle d'accès à l'enregistrement et une clé secrète de relecture KP_c de contrôle d'accès à la relecture.

L'étape 32 consiste à découper, pour chaque flux de données, la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i. Les paquets ainsi constitués sont ensuite appliqués à un module d'embrouillage et de multiplexage 34 qui reçoit parallèlement un message ECM_i contenant les clés de désembrouillage CW_i, CW_{i+1} de contrôle de titre d'accès au contenu du flux et au moins un critère d'accès CA_i, un message $SC\text{-}ECM_i$ contenant les clés de désembrouillage CW_{i-1}, CW_i, CW_{i+1} de contrôle de titre d'accès aux contenu d'un segment S_i de données correspondant à au moins deux crypto-périodes, un

message R-ECM$_c$ contenant la clé d'enregistrement KR$_c$ de contrôle d'accès à l'enregistrement du contenu du segment S$_i$ et au moins un critère CRR définissant un droit à l'enregistrement de ce contenu, et un message P-ECM$_c$ contenant la clé de relecture KP$_c$ de contrôle d'accès à la relecture du contenu du segment S$_i$ enregistré et au moins un critère CRP de contrôle d'accès à la relecture du contenu de ce segment.

Préalablement, à l'étape 36, les clés de désembrouillage CW$_i$, CW$_{i+1}$ sont chiffrées par une première clé secrète de service K$_s$ extraite d'une carte à puce 38, et à l'étape 40, les clés de désembrouillage CW$_{i-1}$, CW$_i$, CW$_{i+1}$ sont chiffrées successivement par la clé d'enregistrement KR$_c$ puis par la clé de relecture KP$_c$, à l'étape 42, la clé KP$_c$ est chiffrée par une deuxième clé de service K'$_s$ extraite de la carte à puce 38, et à l'étape 44, la clé KR$_c$ est chiffrée par la deuxième clé de service K'$_s$.

Les messages ECM$_i$, R-ECM$_i$, P-ECM$_i$ et SC-ECM$_i$ à diffuser sont ensuite appliqués au module d'embrouillage et de multiplexage 34 pour être multiplexés avec le paquet de données et transmis au terminal récepteur.

Notons que l'étape 42 revient à réaliser un sur-chiffrage des mots de contrôle CW$_{i-1}$, CW$_i$, CW$_{i+1}$ successivement au moyen de la clé de relecture KP$_c$, de la deuxième clé de service K'$_s$, puis de la clé d'enregistrement KR$_c$.

Dans une variante de réalisation ce sur-chiffrage des mots de contrôle CW$_{i-1}$, CW$_i$, CW$_{i+1}$ est

réalisé successivement au moyen de la clé K'_s, au moyen de la clé de relecture KP_c, puis au moyen de la clé KR_c.

La figure 3 illustre schématiquement la phase de réception et de désembrouillage d'un contenu diffusé en vue de son enregistrement.

L'étape 50 consiste à rechercher les voies ECM présentes des messages P-ECM_c, R-ECM_c, SC-ECM_i dans la signalisation rattachée au service diffusant le contenu.

L'étape 51 n'est réalisée que si le message R-ECM_c est absent de la diffusion. Une condition supplémentaire est que le terminal récepteur dispose d'un dispositif de commutation bidirectionnelle. L'étape 51 consiste à se connecter à un Serveur d'Autorisation en déclinant l'identifiant du contenu à enregistrer et l'identité du terminal client. Selon des critères connus du Serveur d'Autorisation, ce dernier délivre en ligne le R-ECM_c nécessaire à l'enregistrement du contenu.

A l'étape 52, le message R-ECM_c est présenté au processeur de sécurité qui après vérification des critères d'accès à l'enregistrement mémorise la clé KR_c. L'étape 52 n'est réalisée qu'à condition d'une diffusion du message P-ECM_c.

A l'étape 54, le message P-ECM_c est récupéré puis stocké en l'état dans l'entête du fichier de stockage du contenu.

A l'étape 56, pour chaque crypto-période i, le message SC-ECM_i est récupéré puis présenté au processeur de sécurité qui le déchiffre avec la clé KR_c pour récupérer un message déchiffré SC-ECM_i qui est

ensuite enregistré avec les paquets du multiplex constituant le contenu.

Dans une variante de réalisation, ces paquets du multiplex sont chiffrés localement (étape 58) avec une clé K_I générée à l'étape 60 à partir d'attributs contenus dans le message K-EMC$_c$ et d'un paramètre relatif à l'identité du décodeur. A titre d'exemple, ce paramètre peut être le numéro de série du décodeur, l'identifiant unique (UA) de la carte à puce ou encore le numéro de série d'un disque dur équipant le terminal récepteur.

La figure 4 illustre schématiquement la phase de désembrouillage d'un contenu enregistré dans un support d'enregistrement 60 en vue de sa relecture.

L'étape 62 consiste à rechercher le message P-ECM$_c$ dans l'entête du fichier contenant les données du flux.

L'étape 63 suivante n'est réalisée que si le message P-ECM$_c$ est absent de l'entête du fichier contenant. Une condition supplémentaire est que le terminal dispose d'un dispositif de communication bidirectionnelle. L'étape 63 consiste à se connecter à un Serveur d'Autorisation en déclinant l'identifiant du contenu à lire et l'identité du terminal client. Selon des critères connus du Serveur d'Autorisation, ce dernier délivre en ligne P-ECM$_c$ nécessaire à la lecture du contenu.

A l'étape 64, le message P-ECM$_c$ retrouvé est présenté au processeur de sécurité qui après vérification des critères d'accès à la lecture mémorise la clé de relecture KP$_c$ dans la carte à puce 38.

Si le contenu a été préalablement embrouillé localement conformément à l'étape 58 décrite précédemment, la clé locale d'identité K_I est alors calculée à partir des informations d'identité du terminal récepteur (étape 68), et pour chaque crypto-période i, le multiplex du contenu est déchiffré à la lecture à la volée avec la clé K_I (étape 70).

Dans un mode préféré de réalisation de l'invention, à la relecture, la clé K_I est regénérée à partir d'attributs contenus dans le message P-ECM et d'au moins un paramètre relatif à l'identité du terminal-récepteur et est utilisée pour déchiffrer le contenu enregistré.

A l'étape 72, le message SC-ECM_i courant est récupéré, puis présenté au processeur de sécurité (étape 74) qui le déchiffre avec la clé KP_c pour vérifier les critères d'accès CRP à la relecture et récupérer les mots de contrôle CW_{i-1}, CW_i, CW_{i+1} et la parité de i. Suivant le sens de lecture souhaité, une des clés de désembrouillage ECW ou OCW est fournie au désembrouilleur pour désembrouiller le segment de données S_i.

Dans le cas où le segment S_i doit être visualisé directement, le procédé selon l'invention permet de rechercher la voie ECM et l'indexe des ECM_i dans la signalisation rattachée au service diffusant le contenu à chaque changement de i et d'appliquer l'ECM_i au processeur de sécurité pour récupérer les mots de contrôle pair et impair OCW, ECW et les appliquer au désembrouilleur 80.

ANNEXE 1

Packet IDentifier	Scrambling Control	Payload : Data bytes + padding bytes

Une définition équivalente est

```
CAS_PACKET_UNIT()
{
  Packet IDentifier          x bits ;
  Scrambling_Control         2 bits ;
  Payload  z bytes
}
```

x+2 multiple de 8 ;

La séquence payload sé décompose en Payload()

```
{
 data bytes                  m octets
 padding bytes               p octets
            }
```

ANNEXE 2

```
CA_descriptor()
{
        descriptor_tag = 0x09              8 bits
        descriptor_length                  8 bits
        CA_system_ID                      16 bits
        reserved                           3 bits
        CA_PID                            13 bits
        for (i=0; i<N; i++) {
                private_data_byte          8 bits
```

ANNEXE 3

```
private data bytes ()
{
  Si Voie ECM présente dans le multiplex (voir) :
{
   ECM_CHANNEL_TAG                          1 octet
indicateur de descripteur voie SC_ECM
   ECM_XID ;                                1 octet
indexe de l'ECM Stream dans la voie paquet
   ECM_CI ;                                 1 octet
version du crypto-algorithme  pour l'ECM Stream
   ECM_SOID ;                               3 octets
référence du jeu de clé privé utilisé pour le Stream
}
  Si Voie SC_ECM présente dans le multiplex :
  (                  // Extension du système
    SC_ECM_CHANNEL_TAG                      1 octet
indicateur de descripteur voie SC_ECM
    PPS_ECM_CI;                             1 octet
Version du crypto-algorithme pour les ECM "contenus"
    SC_ECM_SOID;                            3 octets
SOID des SC_ECM
    SC_ECM_PID ;                            x octets
identité de la voie paquet pour les SC_ECM
    SC_ECM_XID ;                            1 octet
indexe du SC_ECM dans la voie paquet

    Si Voie R_ECM présente dans le multiplex :
    {
     R_ECM_CHANNEL_TAG                      1 octet
indicateur de descripteur voie R_ECM
     R_ECM_SOID;                            3 octets
SOID des R_ECM
     R_ECM_PID ;                            x octets
identité de la voie paquet pour les R_ECM
     R_ECM _ XID;                           1 octet
indexe du R_ECM dans la voie paquet
    }

    Si Voie P_ECM présente dans le multiplex :
    {
     P_ECM_CHANNEL_TAG                      1 octet
indicateur de descripteur voie P_ECM
```

```
        P_ECM_SOID;                          3 octets
    SOID des P_ECM
        P_ECM_PID ;                          x octets
    identité de la voie paquet pour les R_ECM
        P_ECM_ XID;                          1 octet
    indexe du P_ECM dans la voie paquet
        }
      }
```

REVENDICATIONS

1. Procédé de contrôle d'accès à un flux de données numériques diffusé et préalablement embrouillé au moyen d'une clé de chiffrement CW transmise sous forme chiffrée dans un message de contrôle de titre d'accès ECM comportant en outre au moins un critère CA de contrôle d'accès, lesdites données numériques étant susceptibles d'être enregistrées telles quelles dans un terminal récepteur ou déchiffrées à la volée, procédé caractérisé en ce qu'il comporte les étapes suivantes :

à l'émission :

- générer un message $R\text{-}ECM_c$ de contrôle de titre d'accès à l'enregistrement du contenu du flux en fonction d'une clé d'enregistrement KR_c et d'au moins un critère CRR définissant un droit à l'enregistrement,
- générer un message $P\text{-}ECM_c$ de contrôle de titre d'accès à la relecture du contenu du flux enregistré en fonction d'une clé de relecture KP_c et d'au moins un critère CRP définissant un droit à la relecture, et

à la réception :

- analyser le message $R\text{-}ECM_c$, et
- autoriser l'enregistrement si le critère CRR est vérifié, sinon, interdire l'enregistrement,
- analyser le message $P\text{-}ECM_c$, et
- autoriser la relecture si le critère CRP est vérifié, sinon, interdire la relecture.

2. Procédé selon la revendication 1, caractérisé en ce que les clés CW, KR_c et KP_c sont chiffrées par une première clé de service K_s.

3. Procédé selon la revendication 1, caractérisé en ce que les clés CW, KR_c et KP_c sont chiffrées par trois clés de service différentes respectivement K_S, K_{SR} et K_{SP}.

4. Procédé selon l'une des revendications 2 ou 3, caractérisé en ce que la phase de l'émission comporte les étapes suivantes :

pour chaque flux de données

- découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i, et à chaque changement de crypto-période,

- embrouiller le contenu du flux au moyen de la clé CW_i, et mémoriser une valeur p(i) représentative de la parité de i,

- calculer un message de contrôle de titre d'accès $SC\text{-}ECM_i$ en fonction des clés de chiffrement CW_{i-1}, CW_i, CW_{i+1} préalablement définies, de la valeur p(i) et du critère CA_i, ledit message $SC\text{-}ECM_i$ étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,

- chiffrer les clés CW_{i-1}, CW_i, CW_{i+1} au moyen de la clé de relecture KP_c,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une deuxième clé de service K'_s,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé d'enregistrement KR_c.

5. Procédé selon l'une des revendications 2 ou 3, caractérisé en ce que la phase de l'émission comporte les étapes suivantes :

pour chaque flux de données :

- découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i, et à chaque changement de crypto-période,

- embrouiller le contenu du flux au moyen de la clé CW_i, et mémoriser une valeur p(i) représentative de la parité de i,

- calculer un message de contrôle de titre d'accès $SC\text{-}ECM_i$ en fonction des clés de chiffrement CW_{i-1}, CW_i, CW_{i+1} préalablement définies, de la valeur p(i) et du critère CA_i, ledit message $SC\text{-}ECM_i$ étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,

- chiffrer les clés CW_{i-1}, CW_i, CW_{i+1} au moyen d'une deuxième clé de service K'_s,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé KP_c,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé d'enregistrement KR_c.

6. Procédé selon les revendications 4 ou 5, caractérisé en ce que la phase de l'émission comporte en outre les étapes consistant :

- calculer le message de contrôle de titre d'accès $ECM_i = f[(ECW_i, OCW_i, CA)]$ où, ECW_i et OCW_i représentent respectivement les mots de contrôle pair et impair préalablement chiffrés au moyen d'une première clé de service K_s,

$ECW_i = CW_i$ si i pair sinon $ECW_i = CW_{i+1}$;

$OCW_i = CW_i$ si i impair sinon $OCW_i = CW_{i+1}$;

- diffuser dans la signalisation ECM des paramètres identifiant les voies ECM rattachées au service diffusant le contenu des messages ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$,

- fournir au terminal récepteur les messages ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$.

7. Procédé selon la revendication 6, caractérisé en ce que les messages ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$ sont diffusés par voies ECM associées au contenu du segment S_i.

8. Procédé selon la revendication 6, caractérisé en ce que, le message R-ECM est délivré au terminal récepteur sur requête à partir d'un Serveur d'Autorisation en tête de réseau.

9. Procédé selon la revendication 6, caractérisé en ce que, le message P-ECM est délivré au terminal récepteur sur requête à partir d'un Serveur d'Autorisation en tête de réseau.

10. Procédé selon la revendication 7, caractérisé en ce que la phase de la réception comporte les étapes suivantes :

- récupérer la voie ECM du message ECM_i à partir de la signalisation rattachée au service diffusant le flux de données, et à chaque changement de i,

- analyser le message ECM_i afin de récupérer les mots de contrôle pair OCW, et impair ECW, pour désembrouiller le contenu du flux diffusé de manière à obtenir un accès direct à ce contenu.

11. Procédé selon la revendication 7, caractérisé en ce que la phase de la réception comporte les étapes suivantes :

- récupérer la voie ECM des messages $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$ à partir de la signalisation rattachée au service diffusant le contenu ;

- analyser le message $R\text{-}ECM_c$ pour vérifier les critères d'accès à l'enregistrement CRR,

- mémoriser la clé d'enregistrement KR_c ;

- récupérer le message $P\text{-}ECM_c$ et le stocker avec le contenu ; et

pour chaque crypto-période i :

- récupérer le message $SC\text{-}ECM_i$,

- déchiffrer le message SC-ECM_i au moyen de la clé d'enregistrement KR_c, et

- enregistrer le message SC-ECM_I déchiffré avec le contenu.

12. Procédé selon la revendication 7, caractérisé en ce que l'accès à la relecture du contenu du flux enregistré est obtenu selon les étapes suivantes :

- récupérer le message P-ECM_c dans le contenu et l'analyser pour vérifier les critères d'accès à la lecture CRP,

- mémoriser la clé de relecture KP_c ; et

- récupérer dans le contenu le message SC-ECM_i courant,

- déchiffrer le message SC-ECM_i avec la clé de relecture KP_c et vérifier les critères d'accès,

- récupérer les clés chiffrés CW_{i-1}, CW_i, CW_{i+1} et la valeur p(i) indiquant la parité de i, et

- déchiffrer lesdites clés suivant le sens de lecture pour en déduire ECW et OCW, puis,

- appliquer soit ECW, soit OCW pour désembrouiller le contenu à la relecture.

13. Procédé selon la revendication 7, caractérisé en ce que l'accès à la relecture du contenu du flux est obtenu selon les étapes suivantes :

- récupérer le message P-ECM_c dans le contenu,

- analyser le message P-ECM_c pour vérifier les critères d'accès à la lecture CRP,

- mémoriser KP_c, et
- récupérer dans le contenu le message $SC\text{-}ECM_i$ courant ;
- déchiffrer le message $SC\text{-}ECM_i$ avec la deuxième clé de service K'_s et vérifier les critères d'accès,
- récupérer les clés chiffrés CW_{i-1}, CW_i, CW_{i+1} et la valeur p(i) indiquant la parité de i, et
- déchiffrer lesdites clés suivant le sens de lecture pour en déduire ECW et OCW, puis,
- appliquer soit ECW, soit OCW pour désembrouiller le contenu.

14. Procédé selon la revendication 11 ou 12, caractérisé en ce que la phase de réception comporte en outre les étapes suivantes :

- générer une clé locale K_I à partir d'attributs contenus dans le message R-ECM et d'au moins un paramètre relatif à l'identité du terminal-récepteur,
- sur-chiffrer localement le contenu à enregistrer par cette clé K_I, et
- à la relecture, regénérer la clé K_I à partir d'attributs contenus dans le message P-ECM et d'au moins un paramètre relatif à l'identité du terminal-récepteur,
- déchiffrer le contenu enregistré au moyen de la clé K_I regénérée.

15. Procédé selon l'une des revendications 1 à 14, caractérisé en ce que les données numériques diffusées représentent des programmes audiovisuels.

16. Système de contrôle d'accès à un flux de données numériques comportant une plate-forme d'embrouillage (2) comprenant au moins un générateur de messages de contrôle de titre d'accès ECM et au moins un récepteur de désembrouillage (4) muni d'un processeur de sécurité (14), caractérisé en ce que la plate-forme d'embrouillage (2) comporte en outre :

- un générateur de messages $R\text{-}ECM_c$ de contrôle de titre d'accès à l'enregistrement du contenu du flux reçu et un générateur de messages $P\text{-}ECM_c$ de contrôle de titre d'accès à la relecture du contenu d'un flux enregistré, et en ce que le récepteur de désembrouillage (4) comporte :

- des moyens pour récupérer la voie ECM des messages $P\text{-}ECM_c$, $R\text{-}ECM_c$,

- des moyens pour déchiffrer le contenu d'un flux reçu pour l'enregistrer, et

- des moyens pour déchiffrer le contenu d'un flux enregistré pour le relire.

17. Système selon la revendication 16, caractérisé en ce que le récepteur de désembrouillage (4) comporte en outre des moyens pour générer une clé locale K_I à partir d'attributs contenus dans le message $R\text{-}ECM_c$ et de l'identité du terminal-récepteur pour chiffrer/déchiffrer localement le contenu du flux reçu.

18. Plate-forme d'embrouillage (2) comportant au moins un générateur de messages de contrôle de titre d'accès ECM à un flux de donnée diffusé sous forme embrouillée, caractérisée en ce qu'elle comporte en outre un générateur de messages $R\text{-}ECM_c$ de contrôle de titre d'accès à l'enregistrement du contenu d'un flux reçu et un générateur de messages $P\text{-}ECM_c$ de contrôle de titre d'accès à la relecture du contenu d'un flux enregistré.

19. Plate-forme d'embrouillage selon la revendication 18, caractérisée en ce qu'elle comporte :

- des moyens pour découper la période d'embrouillage en une suite de crypto-périodes Cp_i définissant chacune une durée de validité d'une clé individuelle CW_i,

- des moyens pour chiffrer le contenu du flux à chaque changement de crypto-période i au moyen de la clé CW_i,

- des moyens pour calculer un message de contrôle de titre d'accès $SC\text{-}ECM_i$ en fonction des clés CW_{i-1}, CW_i, CW_{i+1} correspondant respectivement aux crypto-périodes CP_i, CP_{i-1} et CP_{i+1}, d'un paramètre de parité p(i) et du critère de contrôle d'accès CA_i, ledit message $SC\text{-}ECM_i$ étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,

- des moyens pour chiffrer les clés CW_{i-1}, CW_i, CW_{i+1} au moyen d'une clé de relecture KP_c,

- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une deuxième clé de service K'_s,

- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une clé d'enregistrement KR_c.

20. plate-forme selon la revendication 18, caractérisé en ce qu'elle comporte en outre :

- des moyens pour découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i,

- des moyens pour chiffrer le contenu du flux à chaque changement de crypto-période i au moyen de la clé CW_i,

- des moyens pour calculer un message de contrôle de titre d'accès $SC\text{-}ECM_i$ en fonction des clés CW_{i-1}, CW_i, CW_{i+1} correspondant respectivement aux crypto-périodes CP_i, CP_{i-1} et CP_{i+1}, d'un paramètre de parité p(i) et du critère de contrôle d'accès CA_i, le message $SC\text{-}ECM_i$ étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,

- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une deuxième clé de service K'_s,

- des moyens pour chiffrer les mots de contrôle CW_{i-1}, CW_i, CW_{i+1} au moyen d'une clé de relecture KP_c,

- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une clé d'enregistrement KR_c.

21. Récepteur de désembrouillage (4) d'un flux de donné diffusé sous forme embrouillée par une clé d'embrouillage CW_i comportant un processeur de sécurité comprenant au moins une clé KR_c destinée à désembrouiller des messages $R\text{-}ECM_c$ de contrôle d'accès à l'enregistrement et au moins une clé KP_c destinée à désembrouiller des messages $P\text{-}ECM_c$ de contrôle d'accès à la relecture, récepteur caractérisé en ce qu'il comporte :

- des moyens pour récupérer la voie ECM des messages $P\text{-}ECM_c$ et des messages $R\text{-}ECM_c$ à partir de la signalisation rattachée au service diffusant le contenu ;

- des moyens pour déchiffrer le messages $R\text{-}ECM_c$ au moyen de la clé d'enregistrement KR_c pour vérifier le droit à enregistrer le contenu d'un flux reçu,

- des moyens pour déchiffrer le messages $P\text{-}ECM_c$ au moyen de la clé KP_c pour vérifier le droit à relire le contenu d'un flux enregistré.

22. Récepteur selon la revendication 21, caractérisé en ce qu'il comporte en outre des moyens pour générer une clé locale K_I à partir d'attributs contenus dans le message $R\text{-}ECM_c$ de l'identité du récepteur pour chiffrer et déchiffrer localement le contenu du flux reçu.

23. récepteur selon la revendication 21, caractérisé en ce que le processeur de sécurité est une carte à puce.

ABRÉGÉ DESCRIPTIF

L'invention concerne un procédé de contrôle d'accès à un flux de données numériques diffusé et préalablement embrouillé.

Le procédé selon l'invention comporte les étapes suivantes :

à l'émission :

- générer un message $R\text{-}ECM_c$ de contrôle de titre d'accès à l'enregistrement du contenu du flux en fonction d'une clé KR_c et d'au moins un critère CRR définissant un droit à l'enregistrement,
- générer un message $P\text{-}ECM_c$ de contrôle de titre d'accès à la relecture du contenu du flux enregistré en fonction d'une clé KP_c et d'au moins un critère CRP définissant un droit à la relecture, et

à la réception :

- analyser les messages $R\text{-}ECM_c$ et $P\text{-}ECM_c$,
- autoriser l'enregistrement et la relecture si les critères CRR et CRP sont vérifiés,

FIGURE 2.

SP. 21450

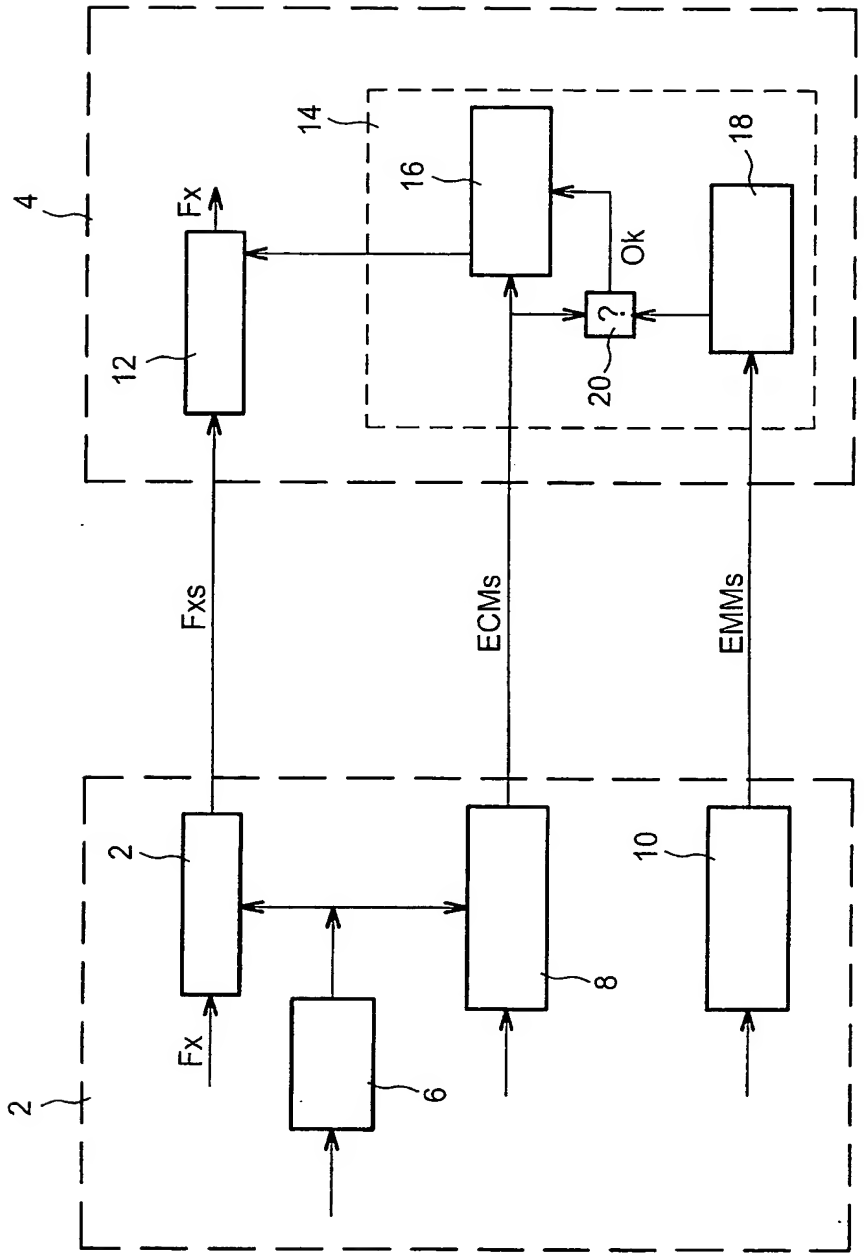

FIG. 1

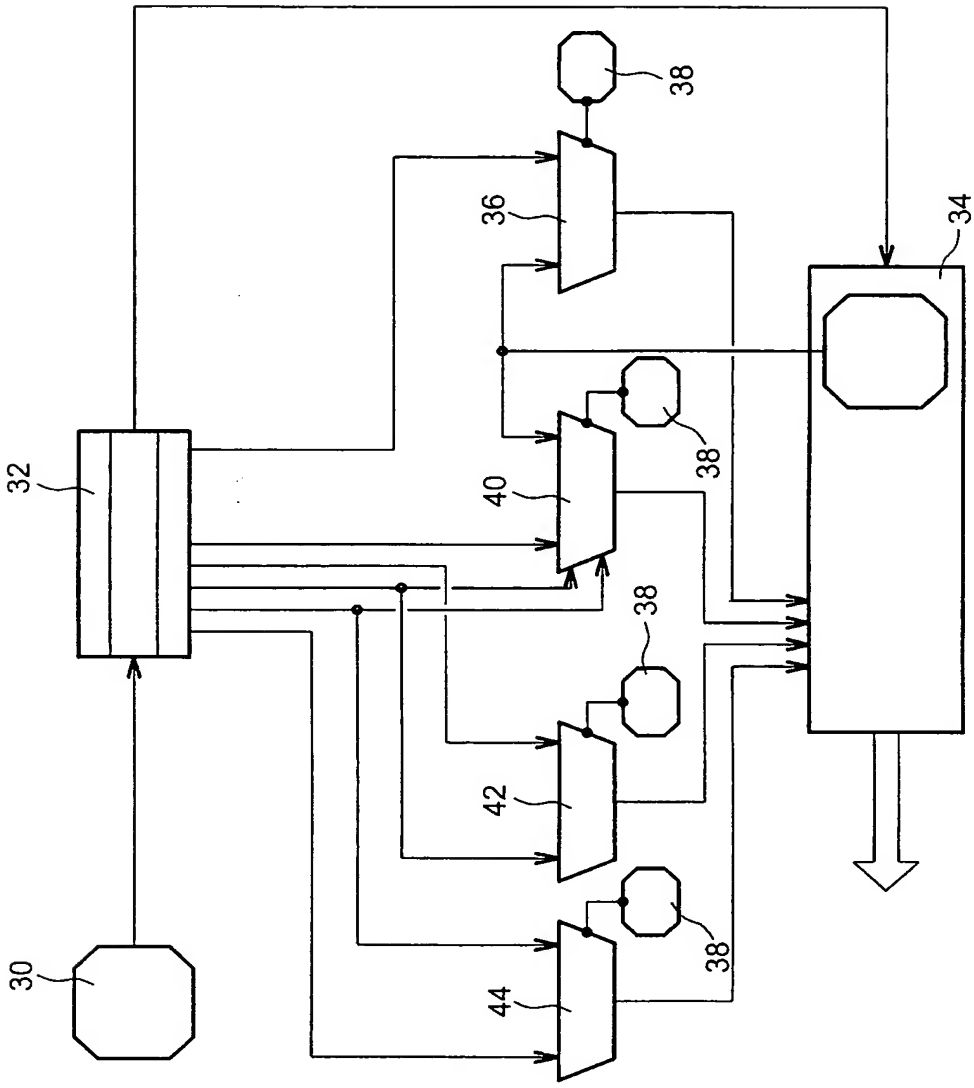

FIG. 2

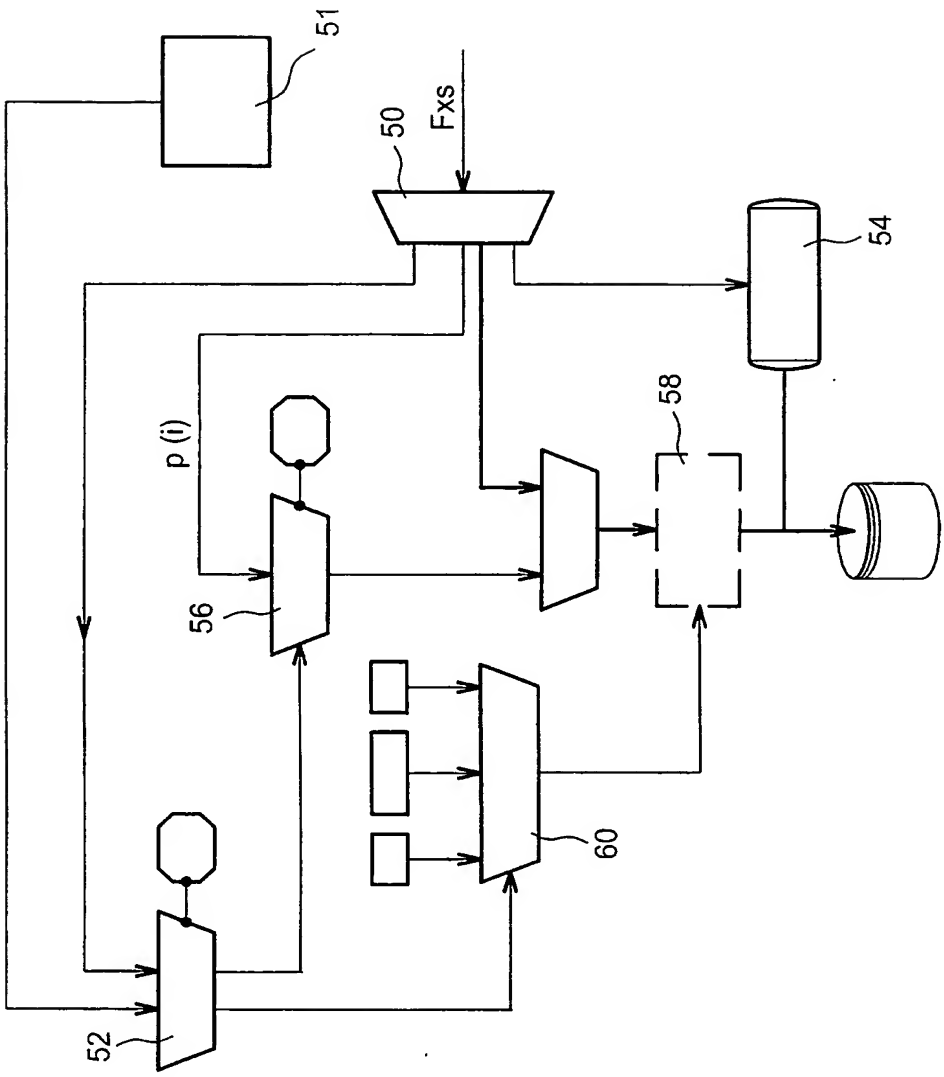

FIG. 3

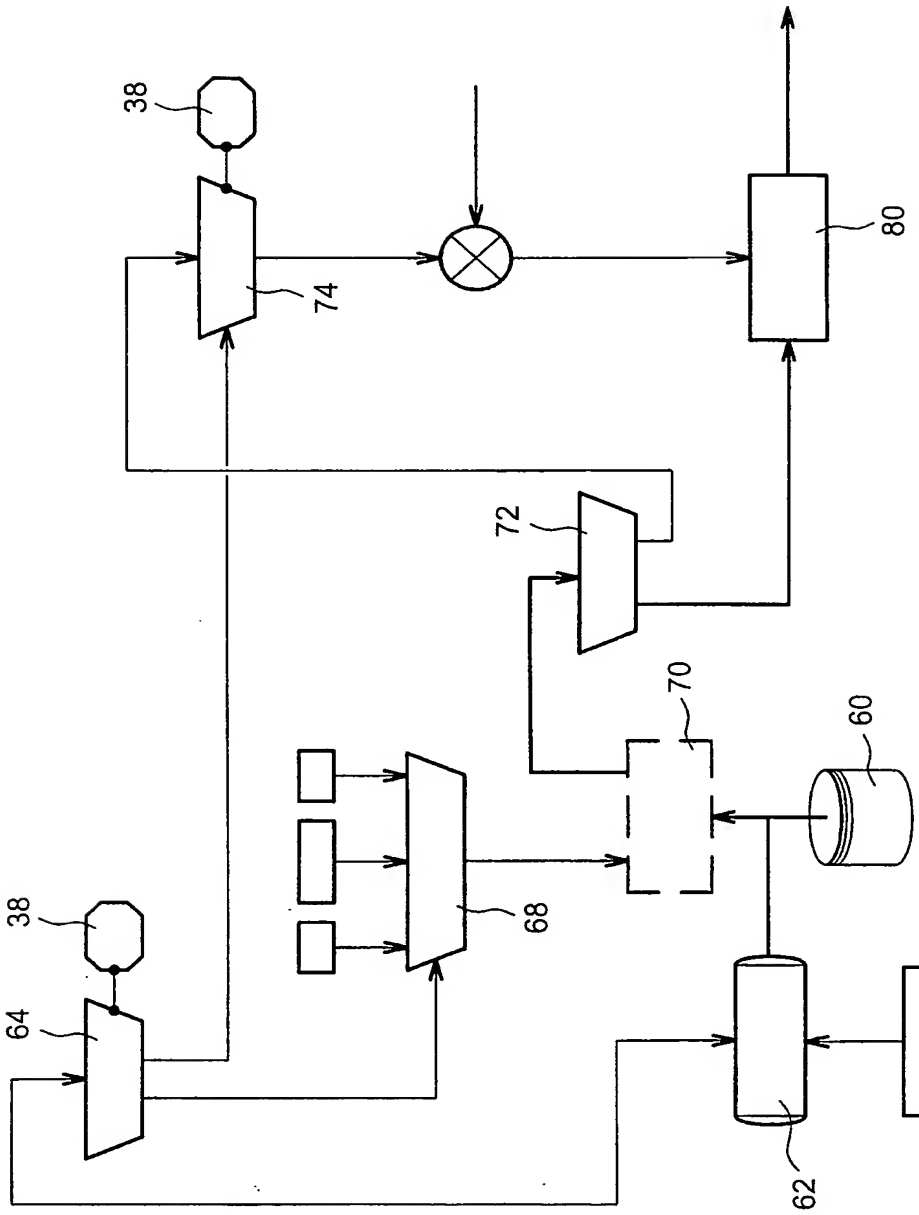

FIG. 4